

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего образования
«Уфимский юридический институт Министерства внутренних дел
Российской Федерации»

Кафедра уголовного-процесса

ДИПЛОМНАЯ РАБОТА

на тему **«ДЕЯТЕЛЬНОСТЬ СЛЕДОВАТЕЛЯ ПО СБОРУ
ДОКАЗАТЕЛЬСТВ, В ТОМ ЧИСЛЕ ПО ПРЕСТУПЛЕНИЯМ В СФЕРЕ
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ
(ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ
ДЕЛ)»**

Выполнил
Младший лейтенант полиции
Садыков Динар Айратович
обучающийся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2018 года набора, 813 учебного взвода

Руководитель
старший преподаватель кафедры
Исанбаев Ильдар Салаватович

К защите _____
рекомендуется / не рекомендуется

Начальник кафедры _____ Е.А. Кулеш
подпись

Дата защиты «__» _____ 2023 г. Оценка _____

ПЛАН

Введение.....	3
Глава 1. Теоретические основы деятельности следователя по сбору доказательств при расследовании преступлений.....	5
§ 1. Следователь как субъект собирания доказательств.....	5
§ 2. Собираение доказательств следователем посредством проведения следственных действий.....	9
§ 3. Собираение доказательств следователем посредством проведения иных процессуальных действий.....	26
Глава 2. Особенности фиксации следственных и процессуальных действий, проводимых с целью получения доказательственной информации, хранящейся на ресурсах сети Интернет.....	30
§ 1. Особенности фиксации хода и результатов изъятия информации, сопряженной с ресурсами сети Интернет.....	30
§ 2. Особенности следственного осмотра и фиксации информации, хранящейся на ресурсах сети Интернет.....	36
§ 3. Компьютерная экспертиза как средство доказывания при расследовании преступлений, совершенных с использованием сети Интернет.....	43
Заключение.....	53
Список использованной литературы.....	55

ВВЕДЕНИЕ

Актуальность выпускной квалификационной работы на тему «Деятельность следователя по сбору доказательств, в том числе по преступлениям в сфере информационно-телекоммуникационных технологий» обусловлена тем, что сбор вещественных доказательств является одним из ключевых этапов уголовного процесса. Вещественные доказательства могут быть физическими объектами, следами преступления, материалами, которые могут быть использованы в судебном разбирательстве для подтверждения вины или невиновности обвиняемого. Точность и надежность собранных доказательств являются фундаментальными для обеспечения справедливого судебного процесса.

Основным субъектом доказывания на предварительном расследовании является следователь – должностное лицо, уполномоченное осуществлять предварительное следствие, а также иные полномочия, предусмотренные законом (п. 41 ст. 5, ст. 38 УПК РФ). Основной задачей следователя являются сбор доказательств в целях установления события преступления, лица, виновного в его совершении, привлечение его в качестве обвиняемого, подготовка условий для судебного разбирательства. Сбор доказательств – это деятельность следователя по обнаружению, получению и закреплению в установленном порядке полученной информации.

Следователь является субъектом доказывания, это и есть несомненный признак должностного лица. Неотъемлемая задача следователя, это сбор и систематизация полученных доказательств в уголовном деле. Несомненно, что качество собранных доказательств, правильное оформление будет полностью влиять на ход предварительного следствия, а в конечном итоге и на судьбу подсудимого. Исходя из вышесказанного, следует, что статус следователя является важным элементом деятельности сотрудника органов внутренних дел.

Объект исследования составляют общественные отношения в процессе осуществления деятельности следователя по сбору доказательств в том числе по преступлениям в сфере информационно-телекоммуникационных технологий.

Предмет исследования составляют нормы уголовного законодательства РФ регламентирующие деятельность следователя по сбору доказательств в том числе по преступлениям в сфере информационно-телекоммуникационных технологий (по материалам территориального ОВД).

Цель исследования: анализ деятельности следователя по сбору доказательств в том числе по преступлениям в сфере информационно-телекоммуникационных технологий (по материалам территориального ОВД).

Задачи исследования:

1. Определить назначение следователя как непосредственный субъект сбора доказательств в уголовном процессе;
2. Рассмотреть процесс собирания доказательств следователем посредством проведения следственных действий;
3. Изучить процесс деятельности следователя по сбору доказательств в процессе исполнения других процессуальных действий;
4. Определить индивидуальность фиксации поэтапность действий следователя и полученных результатов по сбору информации, координированный в сфере сети Интернет;
5. Установить особенности производства осмотра полученной информации и последующей фиксации, которая хранится в просторах сети Интернет;
6. Разобрать понятие что такое компьютерная экспертиза, которая является средством получения доказательств при расследовании уголовного дела, совершенного в просторах сети Интернет.

В содержание работы входит: введение, две главы состоящие каждая из трех параграфов, заключение и список использованной литературы.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ДЕЯТЕЛЬНОСТИ СЛЕДОВАТЕЛЯ ПО СБОРУ ДОКАЗАТЕЛЬСТВ ПРИ РАСЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

§ 1. Следователь как субъект сбора доказательств

Компетенция лиц, осуществляющих уголовное расследование по сбору доказательств регламентированы только в одной статье, а именно ст. 86 УПК РФ¹.

Рассматривая часть первую ст. 86 УПК РФ, в ней содержится информация о субъектах которые правомочны вести процесс по сбору доказательств. Согласно вышеупомянутой статье, сбор доказательств осуществляется дознавателем, следователем, прокурором и судом путем производства следственных и иных процессуальных действий, предусмотренных УПК РФ. Таким образом, следователь, руководитель следственного органа, начальник подразделения дознания, дознаватель собирают доказательства путем производства следственных и иных

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ с внес. изм. от 7 октября 2022 г. № 384-ФЗ // Российская газета. 22 декабря. 2001 г. № 249.

процессуальных действий. При этом к числу иных процессуальных действий относится не только направление следователем, дознавателем и органом дознания требований, поручений и запросов, которые обязательны для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами, но и дача указаний о производстве следственных действий руководителем следственного органа – следователю, а начальником подразделения дознания – дознавателю¹.

В соответствии с российским законодательством следователь уполномочен в пределах компетенции, которой его наделяет УПК РФ, производить предварительное следствие по уголовным делам установленной для него последственности и осуществлять иные полномочия. Следователь независим от кого либо в выборе тактики расследования, так как он является представителем законности, обоснованности и справедливости при производстве уголовного дела. В его обязанности входит полное, всестороннее и объективное обнаружение обстоятельств совершенного преступления, использование полного арсенала уголовно-процессуальных средств и принятие решения по привлечению в случае необходимости дополнительных сил, а так же использование специальных познаний.

Рассматривая данные цели и задачи следователя, появляется необходимость в использовании комплекса необходимых прав и обязанностей, которые реализуются в рамках уголовно-процессуальных правоотношениях, возникающих между всеми участниками уголовного процесса.

Законом предусмотрены положения о принятии следователем самостоятельных решений о использовании какого-либо процессуального действия, если не требуется санкция начальника следственного органа либо же суда.

¹ Манова Н. С., Францифоров Ю. В. Уголовный процесс. Учебное пособие. М.: Юрайт, 2020. С.124.

Процессуальная самостоятельность следователя при этом не изменяется. Выполнение задач следователя на прямую зависит от нормативного регулирования, то есть, при выполнении поставленных задач, следователь следует законам РФ в рамках своих полномочий. Данный аспект раскрывается в практической деятельности следователя, а именно: следователь самостоятельно принимает какое-либо решение о дальнейшем ходе следствия и производство следственных действий (за исключением случаев, когда законом предусмотрено получение санкции суда или согласия руководителя следственного органа) и несет неотвратимую ответственность за их законное и своевременное проведение.

При выполнении своих обязанностей следователь должен руководствоваться моральными принципами-нравственностью, справедливостью. Он должен придерживаться правовых начал и личных убеждений, которые не должны противоречить законодательству Российской Федерации.

Среди моральных принципов, которыми должен руководствоваться следователь в своей деятельности, можно выделить следующие:

- честность и беспристрастность в отношении всех участников уголовного процесса;
- уважение к правам и интересам граждан, а также соблюдение их конфиденциальности;
- соблюдение процессуальной независимости и неприкосновенности экспертизы;
- соблюдение принципа непротиворечивости и достоверности доказательств;
- обеспечение соблюдения установленных законом сроков и правил при расследовании уголовных дел.

Если в расследовании уголовного дела участвует следственная группа, ответственность за непосредственное расследование несет сотрудник, который принял уголовное дело к своему производству. Все члены

следственной группы имеют равные права, предусмотренные уголовно-процессуальным кодексом.

Взаимодействие следователя и эксперта в доказывании уголовных дел может привести к некоторым проблемам, например:

Несоответствие компетентности эксперта требованиям уголовного дела. Если эксперт не имеет достаточной компетенции в данной области, его результаты могут быть неточными или недостаточно обоснованными.

Нарушение принципа независимости экспертизы. Если следователь оказывает давление на эксперта или влияет на процесс проведения экспертизы, это может отразиться на результате искажении фактов и нарушении принципа независимости экспертизы.

Проблемы с правами эксперта. Если эксперту не предоставляются все необходимые условия для работы (например, доступ к материалам дела), он может не быть в состоянии выполнить свою работу на должном уровне.

Возможность злоупотребления правом эксперта на сбор доказательств. Если эксперту предоставляется право на сбор доказательств, это может привести к необоснованным злоупотреблениям и нарушению принципа законности в уголовном судопроизводстве.

Важно отметить, что право на сбор доказательств должно оставаться за лицом, ответственным за уголовное дело, чтобы предотвратить возможные нарушения и злоупотребления. Следователь должен работать в тесном сотрудничестве с экспертом, но при этом не оказывать на него давления и обеспечивать его независимость в процессе проведения экспертизы¹.

По данному вопросу существует два варианта разрешения. Первый вариант предполагает, что следователь должен проводить осмотр микрообъектов на месте их обнаружения, индивидуализирующие признаки должны фиксироваться в протоколе проводимого следственного действия,

¹ Пивоварова А. О. Проблемы собирания доказательств субъектами доказывания в уголовном судопроизводстве // Молодой ученый. 2018. № 27. С. 110–113.

после чего микрообъекты приобщаются к уголовному делу в качестве вещественных доказательств и направляются на экспертизу. Второй вариант предполагает, что в исследовании участвует не менее двух экспертов, если имеется гипотеза о наличии микрообъектов.

Первый вариант является более эффективным, так как позволяет использовать инструментальную базу для производства следственного действия и получить более точные результаты. Однако, следователь должен присутствовать при производстве экспертизы для возможности обнаружения доказательственной информации.

Второй вариант вызывает сомнения, так как требует от эксперта выполнения роли в собирании доказательств, что не соответствует нормам уголовно-процессуального кодекса. При этом, следователь не может вмешиваться в процесс исследования эксперта.

В законе на должном уровне не регламентированы вопросы, связанные с юрисдикцией субъектов при назначении экспертизы. Однако, в некоторых случаях будет правильным обязать следователя или дознавателя принимать участие в проведении экспертизы для возможности процессуального закрепления обнаруженной доказательственной информации.

Участие следователя при вскрытии трупа является целесообразным для установления причин смерти. Внешний осмотр трупа на месте происшествия производит следователь с участием понятых и врача-специалиста в области судебной медицины, а при невозможности его участия иного врача¹.

§ 2. Собираание доказательств следователем посредством проведения следственных действий

¹ Ромашко, А. Н. Место следователя среди субъектов доказывания в уголовном процессе / А. Н. Ромашко. Текст : непосредственный // Новый юридический вестник. 2020. № 1. С. 29-32.

Главным способом собирания и проверки доказательств в стадии предварительного расследования является производство следственных действий.

Следственные действия – это совокупность действий нацеленные на обнаружение, собирание и проверку доказательств, которые урегулированы уголовно-процессуальным законом.

Правомочен проводить следственное действие, только тот сотрудник, в производстве которого находится уголовное дело. Но так же немаловажен факт, что на основании поручения следователя следственные действия могут проводить органы дознания или другие следователи.

Самое главное основание для производства следственных действий это, наличие возбужденного уголовного дела. Существует исключение из правил, а именно для осмотра места происшествия, освидетельствования и назначения экспертизы, которые могут быть проведены до возбуждения уголовного дела.

Для производства следственных действий необходимо наличие оснований, те фактические данные, которые указывают на необходимость производства тех или иных следственных действий.

Как правило, следственные действия производятся по инициативе следователя или лица, производящего дознание. Но они могут быть произведены и по указанию прокурора, начальника следственного отдела, начальника органа дознания. Кроме того, закон устанавливает случаи обязательного производства следственных действий.

К следственным действиям относятся: допрос; очная ставка; осмотр; освидетельствование; обыск; выемка; предъявление для опознания; следственный эксперимент; наложение ареста на почтово-телеграфные отправления, их осмотр и выемка; контроль и запись переговоров; проверка показаний на месте; назначение и производство экспертизы.

Большинство авторов относят к следственным действиям следующее: наложение ареста на имущество; эксгумация трупа, получение образцов для

сравнительного исследования; помещение лица в медицинское учреждение для производства экспертизы.

Обращая внимание на рассмотренные следственные действия, можно сделать вывод, того что они не могут считаться следственными в прямом смысле. Тем не менее названные действия тесно связанные к следственным, они подготавливают и обеспечивают их производство в целях получения новых доказательств.

При производстве следственных действий следователь является представителем обеспечения охраны прав и интересов граждан. Нормативно правовые акты регулирующие деятельность следователя, предписывают правила производства предварительного следствия, а именно запрещается в процессе собирания доказательств совершать действия, унижающие честь и достоинство граждан или связанные обстоятельства с опасностью для жизни и здоровья. При проведении следственных действий не допускается применение насилия, угроз и иных незаконных мер; нельзя производить следственные действия в ночное время, кроме случаев, не терпящих отлагательства.

При производстве следственных действий должны соблюдаться меры по охране имущества, государственной тайны, а также не разглашение сведений об интимных сторонах жизни участвующих в них лиц.

Следующие следственные действия, такие как освидетельствование, обыск, выемка, экспертиза, эксгумация производятся на основании постановления следователя. Для проведения иных следственных действий вынесения постановления не требуется. Процесс, итоги полученные в результате следственного действия заносятся в протокол. Составление протокола происходит в течении проведения самого следственного действия или после его окончания.

Анализируя УПК РФ можно сделать вывод, что следственным действиям посвящены многие статьи (ст. 40, 65, 83, 86, 141, 146, 149, 152, 157, 164 – 167 и т.д.), однако отсутствует общее понятие, что такое следственное

действие. Но так же ст. 5 УПК РФ, посвященная основным понятиям УПК РФ, не содержит определение понятия «следственное действие», но раскрывает значение термина «неотложные следственные действия» – это «действия, осуществляемые органом дознания после возбуждения уголовного дела, по которому производство предварительного следствия обязательно, в целях обнаружения и фиксации следов преступления, а также доказательств, требующих незамедлительного закрепления, изъятия и исследования (п. 19 ст. 5) и «процессуальные действия», куда относит «следственное, судебное или иное действие, предусмотренное настоящим Кодексом» (п. 32 ст. 5).

Полагая, что уточнение сущности понятия собирания доказательств позволит сформулировать определение следственных действий.

Законодатель не дает точного определения понятию «собрание доказательств» в целом и в рамках следственных действий в частности. Нет единого мнения по этому вопросу и у правоведов. При этом так же, как и по процессу доказывания, до настоящего времени отсутствует единая точка зрения на природу доказательств, что в немалой степени усложняет задачу исследователей в определении процесса собирания доказательств. По вопросу собирания доказательств В. Я. Дорохова приводит мнение, с которым, на наш взгляд, следует согласиться: «Собрание доказательств – процессуальная деятельность органов дознания, следователя, прокурора и суда, направленная на обнаружение фактических данных и их процессуальное оформление»¹.

Особое внимание следует обратить на тот факт, что законодатель объединяет полученные показания только с таким следственным действием, как допрос. Однако показания могут формироваться и в ходе очной ставки, поскольку сущность последней заключается в получении устной информации путем одновременного допроса двух лиц. Рассматривая данный вопрос следует отметить, что показаниями подозреваемого, обвиняемого, свидетеля и потерпевшего, гражданского истца и гражданского ответчика являются

¹ Дорохов В. Я. Природа вещественных доказательств // Актуальные проблемы российского права. 2017. №18. С.234-239.

сведения, зафиксированные в протоколах допроса и очной ставки, а сообщения этих участников уголовного процесса, сделанные в ходе иных следственных действий, содержатся в таком источнике, как протоколы следственных действий.

Предполагаю, что собирание доказательств – это:

1) деятельность, нацеленная на сбор необходимого количества доказательств;

2) этап накопления количества доказательств, окончанием которого является переход к качественной их обработке – оценке и проверке в соответствии со свойствами доказательств (допустимость, относимость, достоверность, достаточность).

Также необходимо отметить, что рассмотрение ряда спорных вопросов теории доказательств позволяет сделать вывод, что собирание доказательств, получение доказательственного материала составляют основу доказывания, процесса расследования и следственных действий, под которыми мы понимаем разновидность процессуальных действий, производимых с целью собирания и оценки доказательств уполномоченными органами.

Подводя итог вышесказанному, считаю необходимым уточнить содержание ст. 86 УПК РФ в части терминологического определения собирания доказательств:

«Первый этап собирания доказательств заключается в собирании доказательств, который осуществляется в ходе уголовного судопроизводства следователем, дознавателем, а также в следствии производства следственных и иных процессуальных действий предусмотренные УПК РФ».

Следственные действия являются основной частью уголовно-процессуальной деятельностью следователя. Следственные действия – это регламентированные уголовно-процессуальным законом процессуальные действия по собиранию и проверке доказательств, проводимые уполномоченными на то лицами с целью установления и доказывания имеющих значение для уголовного дела фактических обстоятельств,

характеризующиеся детальной процедурой производства и оформления, обеспеченные уголовно-процессуальным принуждением¹.

Возьмем, к примеру, наблюдение, оно в уголовно-процессуальном контексте является крайне важным и неотъемлемым элементом справедливого судопроизводства. Оно играет решающую роль в обеспечении прозрачности, общественного контроля и защиты прав и интересов сторон, участвующих в уголовном процессе.

Наблюдение в уголовно-процессуальном контексте - это процесс визуального восприятия обстановки, имеющей криминалистическое значение, а также их соответствующая фиксация. В теории наблюдение делится на два типа: включенное и невключенное. Включенное наблюдение предполагает контакт исследователя с членами микрогруппы, в то время как невключенное наблюдение заключается в регистрации фактов и событий, без вмешательства в их развитие.

Несмотря на то, что наблюдение обычно считается объективным методом получения информации, следует помнить, что оно также может быть подвержено влиянию субъективных факторов. Например, сознание исследователя может повлиять на то, как он интерпретирует данные, полученные в результате наблюдения, что может привести к искажению результатов исследования. Поэтому необходимо строго выполнять требования системности, активности, целенаправленности и подготовленности при проведении наблюдения.

В целом, наблюдение является важным инструментом в уголовно-процессуальной практике, который может помочь выявить факты и события, имеющие значение для расследования преступлений. Однако, при его использовании следует помнить об ограничениях метода и не допускать субъективных искажений результатов наблюдения.

¹ Халили У. Д. Понятие следственных действия и их место в системе процессуальных действий // Правовестник. 2018. № 6. С. 17 -24.

В целях минимизации негативных последствий при использовании тактического приема «наблюдение», исследователь должен тщательно подготовиться к выполнению этого приема. Далее приведены несколько рекомендаций, которые могут помочь в этой подготовке:

- собрать как можно больше сведений об объекте наблюдения. Это позволит узнать больше о характеристиках объекта, поведении и привычках людей, которых предстоит наблюдать;

- четко определить цели и задачи наблюдения и составить план или схему его проведения. Это поможет исследователю быть нацеленным на конкретные цели и избежать случайных отклонений от них;

- принимать меры к отысканию не только того, что предполагается обнаружить, но и обратного тому. Это поможет исследователю не упустить никаких деталей и получить точную картину происходящего;

- быть готовым к тому, что воспринимаемые признаки могут быть специально подготовленной (ложной) демонстрацией или инсценировкой. Исследователь должен быть готов к тому, что возможно, обнаружение ложных сведений и изменения в поведении;

- проанализировать результаты ранее проведенных наблюдений (если имеются). Это поможет исследователю понять, какие методы были эффективны, а какие - нет, и использовать этот опыт при проведении нового наблюдения;

- обеспечить участие специалистов соответствующего профиля при необходимости, подготовить для них материалы, сформулировать вопросы и т. д. Это поможет получить более точные данные и проанализировать их объективно.

Соблюдение этих рекомендаций поможет исследователю провести наблюдение таким образом, чтобы получить максимально возможное количество информации и минимизировать возможность ошибок¹.

¹ Скобелкина К. С. Следственные действия, основанные на визуальных наблюдениях и опытных действиях // Трибуна ученого. 2020. № 2. С. 130 -138.

Рассмотрим более подробно методы собирания информации с помощью визуального наблюдения. Визуальное наблюдение - это метод сбора информации, который позволяет собирать данные относительно поведения, внешности и окружающей обстановки. Он может применяться в различных контекстах, таких как обыски и проверки, а также при проведении исследований.

При наблюдении за людьми в рамках тактики обыска можно получить некоторую информацию о их психологическом состоянии и действиях. Наблюдение за мимикой лица, жестами рук, положением туловища и другими физическими признаками может предоставить некоторые подсказки о внутренних состояниях и намерениях наблюдаемых лиц.

Например, увеличение напряжения или нервозности в определенных ситуациях может указывать на потенциальное нарушение или сокрытие чего-либо. Изменения в поведении, такие как частое касание лица, ручек, непроизвольные движения или покраснение кожи могут свидетельствовать о тревоге или нервозности.

Кроме того, визуальное наблюдение может быть полезным и при проведении проверки показаний на месте. В результате наблюдения можно собрать данные, которые будут использованы для анализа достоверности показаний.

Как обоснованно отмечает С.С. Арсентьева, «в ходе проверки показаний на месте следователь, либо по его поручению оперативный работник, осуществляют постоянное наблюдение за состоянием и поведением человека, чьи показания проверяются. Это позволяет судить о том, уверенно или нет он действовал в ходе проверки, каким было его эмоциональное состояние как в целом, так и в тем или иные моменты следственного действия, с чем связано изменение состояния»¹.

¹ Арсентьева С. С. Проверка показаний на месте: криминалистический анализ следственного действия, этические аспекты уголовно - процессуальной деятельности проверки и оценки данного доказательства // Российский судья. 2020. № 2. С. 27 - 32.

В контексте конкретных следственных действий, такой как допрос, тактический прием «наблюдение» может быть очень полезным для выявления изменений в поведении и состоянии допрашиваемого. Этот прием позволяет фиксировать множество явлений, происходящих вокруг наблюдателя, и выделить различные взаимосвязи, что может помочь в выявлении неправдивых показаний или скрытых фактов.

Однако, необходимо иметь в виду ограничения данного приема: он позволяет наблюдать только за тем, что можно увидеть объективно, то есть за поведением человека. Вербальное поведение (речь), невербальное поведение (мимика лица, экспрессия тела, выразительность жестикуляции), особенности передвижения в пространстве, поза и другие аспекты поведения могут быть источником информации для наблюдателя.

Для эффективного использования тактического приема «наблюдение» необходимо обладать устойчивым вниманием и способностью концентрироваться на объекте наблюдения без отвлечения на другие факторы. Это требует определенной сноровки и опыта, и формирование рефлексивного мышления может играть важную роль в данном процессе.

Таким образом, при использовании тактического приема «наблюдение» в рамках конкретных следственных действий необходимо учитывать его ограничения и требования к наблюдателю, чтобы достичь максимальной эффективности и получить максимум информации.

Так же следует помнить, что эффективность применения данного приема напрямую зависит от способности наблюдателя к анализу поведения и интерпретации полученной информации. При использовании тактического приема, а именно как «наблюдение» при проведении допроса и очной ставки, необходимы навыки и знания для правильного интерпретирования полученной информации.

Непосредственное наблюдение является важным тактическим приемом в процессе допроса и проведения следственного эксперимента из-за нескольких причин:

Оценка показаний: Наблюдение за действиями и выражением лица допрашиваемого может помочь правильно оценить даваемые им показания. Например, если допрашиваемый рассказывает о чем-то, что должно вызвать у него эмоциональную реакцию, но его лицо остается без каких-либо изменений, это может указывать на то, что он лжет.

Замечание улики: Наблюдая за действиями допрашиваемого, можно заметить улики поведения, которые могут помочь расследованию. Например, если допрашиваемый неожиданно меняет свою позу или начинает шевелиться, когда говорит о чем-то конкретном, это может указывать на то, что он скрывает что-то важное.

Корректировка процесса допроса: Наблюдение позволяет детально следить за процессом допроса и вносить коррективы в него, если это необходимо. Например, если допрашиваемый начинает вести себя агрессивно или нервничать, можно изменить тактику допроса для того, чтобы сохранить контроль над ситуацией.

В целом, непосредственное наблюдение является неотъемлемой частью процесса допроса и следственного эксперимента, которое помогает получить более точные и полезные данные при расследовании преступлений.

Наблюдение также влияет на выбор и применение других тактических приемов. Кроме того, оно позволяет исследовать объект с разных точек зрения, учитывая изменяющиеся ситуации и условия наблюдения.

Хотя результаты наблюдения не заносятся в протокол следственного действия, они могут помочь правильно оценить ситуацию и принять верные решения. В целом, непосредственное наблюдение является важным инструментом для сбора информации и проведения успешного следственного действия¹.

Также, процесс модернизации системы следственных действий является сложным и длительным как с научной, так и с практической точки зрения. Это

¹ Коновалова А. Б., Гук А. Г. Следственные действия как способы собирания доказательств в досудебном производстве// Студент. 2021. №143. С. 59-64.

может означать, что научные исследования могут потребоваться для разработки новых методов опознания или изменения существующих методов, чтобы они были более эффективными и справедливыми.

Таким образом, необходимость постоянного развития уголовно-процессуального законодательства и системы следственных действий, чтобы они соответствовали современным вызовам и требованиям правосудия.

Для того, чтобы познавательный прием стал самостоятельным следственным действием, закрепленным в уголовно-процессуальном законе, он должен пройти несколько этапов становления.

Первый этап разработки нового метода познания - это обнаружение потребности в нем. Это может произойти по нескольким причинам:

Недостаточная эффективность существующих методов: Если существующие методы расследования или сбора доказательств не дают достаточно хороших результатов, то это может привести к поиску новых методов.

Новые виды преступлений: Появление новых видов преступлений, таких как киберпреступления, может потребовать разработки новых методов расследования и сбора данных.

Необходимость более точных данных: В некоторых случаях могут потребоваться более точные данные для расследования преступлений или судебного процесса. Например, в процессе ДНК-анализа, требуется высокий уровень точности, поэтому могут быть разработаны новые методы сбора данных для улучшения точности.

Обнаружение потребности в новом методе познания может стать отправной точкой для проведения исследований и разработки новых методов расследования и сбора данных, которые будут более эффективными и удобными для использования в полицейской работе и других областях правопорядка.

Второй этап разработки нового метода познания - это его внедрение в рамках процессуальных действий, предусмотренных законом. Это означает,

что метод должен быть законным и соответствовать правилам сбора и использования доказательств.

Если потребность в новом методе возникла в ходе допроса свидетелей, следователи могут использовать этот прием при допросе свидетелей. Такой метод может помочь привлечь к ответственности виновных лиц или обеспечить больше доказательств в пользу определенного подозреваемого.

Однако, для использования нового метода познания в рамках процессуальных действий, он должен быть законным и соответствовать всем требованиям, установленным законом. Например, если новый метод является техническим средством, например, программным обеспечением для анализа данных, то его использование может подвергаться ограничениям, установленным законами на защиту конфиденциальности и личных данных.

Второй этап направлен на разработку нового метода познания предполагает не только создание нового метода, но и его проверку на соответствие законодательству и разрешение его использования в рамках процессуальных действий.

Третий этап разработки нового метода познания - это теоретическое обобщение практики и определение целесообразности нормативной регламентации нового приема. На этом этапе после внедрения нового метода происходит его тестирование на практике. В результате проведенных испытаний, правоведы проводят анализ результатов использования нового метода и дают свое заключение относительно его эффективности и целесообразности.

Определение целесообразности нормативной регламентации нового приема предполагает решение вопросов, связанных с возможными ограничениями в использовании метода, установлением требований к квалификации специалистов, занимающихся применением метода, а также соответствующим объяснением положений закона, которые регулируют применение нового метода.

В целом, третий этап является важным для разработки нового метода познания, так как он помогает определить целесообразность его использования в реальной практике и дает возможность принять меры по регулированию его использования в соответствии с законодательством.

Последний этап предусмотрен законодательством и считается новым. В закон вносятся новые правила, которые регламентируют использование нового приема, как самостоятельного следственного действия.

Процесс легализации нового следственного действия является длительным и трудоемким, но он является необходимым для обеспечения справедливости и эффективности уголовного процесса.

Новый метод расследования, который не соответствует требованиям закона, может привести к нарушению прав подозреваемых или обвиняемых, а также к неправильному принятию решения в суде. Поэтому, любой новый метод должен строго соответствовать законодательству и быть законным.

Кроме того, процесс легализации нового следственного действия позволяет убедиться в его эффективности и доказать, что новый метод является более эффективным, чем существующие методы. Это помогает усилить доказательную базу в уголовном деле и повысить вероятность вынесения справедливого решения.

Некоторые из ныне существующих следственных действий, как справедливо указывается в юридической литературе, требуют определенных дополнений, расширений, отдельного внимания со стороны законодателя¹. Хорошим примером будет являться контроль и запись переговоров, регламентированный ст. 186 УПК РФ, ведь оно действительно не является полностью эффективным способом сбора доказательств из-за возможности передачи информации в знаковой или кодированной форме.

¹ Елагина Е. А. Перспективы развития системы следственных действий // Сборник научных статей 3-й Международной научной конференции студентов и молодых ученых. - Курск: Закрытое акционерное общество Университетская книга, 2018. -С. 159- 162.

Быстрое развитие информационных технологий и новые способы передачи информации представляют вызов для следственных органов. Чтобы эффективно собирать доказательства в современном мире, следует использовать новые методы.

Например, следственные органы могут использовать цифровую форензику, которая позволяет изучать данные на компьютерах, мобильных устройствах и других электронных устройствах. Среди таких данных могут быть текстовые сообщения, фотографии, видео- и аудиозаписи, а также файлы социальных сетей и прочие. Эти данные могут быть полезными доказательствами в уголовных делах.

Кроме того, следственные органы могут использовать аналитические инструменты для обработки больших объемов данных. Такие инструменты позволяют автоматически анализировать большое количество информации, выявлять связи между различными элементами и выделять ключевые факты.

Наконец, следственные органы могут использовать средства массовой информации для поиска свидетелей и получения дополнительной информации о преступлениях. Социальные сети, блоги и другие онлайн-платформы могут быть полезными инструментами для сбора информации и свидетельских показаний.

В целом, следственные органы должны учитывать быстрое развитие информационных технологий и использовать новые методы и инструменты для сбора доказательств. Только так они смогут эффективно бороться с преступностью в современном мире.

Такое действие следователя является целесообразным и соответствует требованиям законодательства. При копировании информации с электронных носителей, следует учитывать технические особенности каждого носителя. Следователь должен указать в протоколе следственного действия все используемые технические средства, включая программное обеспечение, которое использовалось при копировании информации.

В протоколе следственного действия следует указать порядок применения технических средств, например, если были использованы программы для скрытого копирования информации, то этот факт также должен быть отражен в протоколе.

Кроме того, следует указать все электронные носители информации, к которым были применены технические средства, и полученные результаты. Важно отметить, что необходимо сохранять оригинальные электронные носители информации, а не только их копии.

Копии электронных носителей информации, содержащие скопированную информацию, также должны прилагаться к протоколу следственного действия. Копии этих носителей могут использоваться в качестве доказательств в уголовном процессе.

В целом, следователь должен придерживаться всех требований законодательства и правил сбора и хранения доказательств. Указывая все используемые технические средства и сохраняя оригинальные электронные носители информации, он обеспечивает юридическую значимость полученных доказательств.

Так же в уголовно-процессуальном кодексе существует пробел, а именно, что не регламентировано следственное действие-проверка показаний на полиграфе. Предполагается, что данное следственное действие будет представлять проведение по решению следователя специалистом-полиграфологом психофизиологического исследования с использованием полиграфа в целях проверки сведений, сообщенных ранее подозреваемым (обвиняемым), потерпевшим или свидетелем в ходе допроса, очной ставки, предъявления для опознания, проверки показаний на месте. Производство психофизиологического исследования возможно при наличии письменного

согласия участника уголовного судопроизводства, чьи показания проверяются¹.

В ходе следственного процесса с участниками могут проводиться различные методы исследования, в том числе, психофизиологическое исследование с помощью полиграфа. По результатам такого исследования, специалист-полиграфолог оформляет письменный документ, который может быть использован как один из видов доказательств в уголовном процессе.

Однако следует отметить, что наличие результатов психофизиологического исследования, проведенного с помощью полиграфа, не является основанием для вынесения приговора или решения по делу. Результаты такого исследования не должны рассматриваться как окончательное доказательство в уголовном деле.

Специалист-полиграфолог должен составить письменный документ, отражающий все факты и обстоятельства, выявленные в ходе исследования. В этом документе должны быть указаны не только результаты исследования, но и методика, примененная при проведении исследования, а также возможные ошибки и ограничения данного метода.

Во время исследования участника процесса, ему задаются тестовые вопросы, могут быть предъявлены материальные доказательства и документы. Результаты психофизиологического исследования, проводимого специалистом-полиграфологом, оформляются в письменном виде. Так же специалист, может быть допрошен для дачи более конкретных объяснений по итогу проведенного исследования. Следует отметить, что различные методы усовершенствования системы следственных действий зависят от общего развития уголовного судопроизводства. При этом характерно выделение тех познавательных действий, которые направлены на определенный обособленный объект или основаны на какой-либо специфической операции.

¹ Сафронов Д. М. Уголовно-процессуальные и криминалистические аспекты получения информации о пользователях сети Интернет при производстве следственных действий // Российская юстиция. - 2021. - № 1. - С. 30 - 33.

Новые технологии и информационные ресурсы позволяют проводить более эффективное расследование преступлений и сокращать время, необходимое для сбора доказательств. В связи с этим появляются новые виды следственных действий, например, изыскание данных о местоположении устройства или получение информации из Общероссийского федерального реестра юридических лиц.

Однако, при создании новых видов следственных действий следует учитывать соответствие таких действий конституционным правам граждан, а также защите персональных данных. Кроме того, необходимо разработать четкую методику использования всех видов следственных действий, чтобы предотвратить возможность злоупотребления и нарушения прав граждан.

Поэтому законодатель должен обеспечивать правовую защиту граждан, устанавливая четкие правила и процедуры для осуществления каждого вида следственного действия. Законодатель должен также обеспечивать контроль за использованием новых технологий и информационных ресурсов, чтобы предотвратить нарушения прав граждан.

В целом, увеличение количества самостоятельных видов следственных действий требует повышенного внимания со стороны законодателя. Необходимо создавать новые виды следственных действий с учетом конституционных прав граждан и персональных данных, а также обеспечивать правовую защиту граждан при использовании новых технологий и информационных ресурсов.

Нельзя не отметить, что в ряде следственных действий участие сведущих лиц является императивным требованием закона. Так, обязательное участие педагога или психолога в допросе несовершеннолетнего подозреваемого и обвиняемого предусмотрено ст. 425 УПК РФ, обязательное участие педагога в допросе несовершеннолетнего свидетеля и потерпевшего - ст. 191 УПК РФ, врача при осмотре трупа - ч. 1 ст. 178 УПК РФ и освидетельствовании - ч. 4 ст. 179 УПК РФ. О тождественности правового статуса специалиста, врача, психолога, педагога, как правильно отмечает

Е. А. Семенов, свидетельствует детальный анализ отдельных положений УПК РФ, и привлекать к участию в производстве следственных действий указанных лиц следует по правилам ст. 58 УПК РФ.¹ Таким образом, дальнейшее развитие системы следственных действий напрямую зависит от выбора законодателем пути совершенствования уголовного судопроизводства в целом.

§ 3. Собираание доказательств следователем посредством проведения иных процессуальных действий

УПК РФ не содержит точного определения понятия «иные процессуальные действия», что может приводить к недостаточной ясности и остроте в решении судебных дел. Кроме того, отсутствие конкретного перечня этих действий и описания порядка их проведения может усложнять сбор информации и снижать эффективность уголовного процесса.

Однако, следует отметить, что УПК РФ предусматривает возможность использования иных процессуальных действий по решению следователя или суда в случаях, когда это необходимо для выявления и раскрытия преступления. Таким образом, иные процессуальные действия могут быть использованы только при наличии законных оснований и в соответствии с требованиями уголовно-процессуального законодательства.

В то же время, для повышения эффективности уголовного процесса и обеспечения единства правоприменения, законодатель может разработать конкретный перечень иных процессуальных действий и описать порядок их проведения. Это позволит установить четкие правила и процедуры для использования таких действий, а также обеспечит единообразное применение закона на всей территории России.

¹ Семенов Е. А. Правовое положение некоторых неуказанных в гл. 5-8 УПК РФ субъектов уголовного судопроизводства России. - М.: НОРМА, 2020.- С.101.

Поэтому, следует рассмотреть вопрос о введении конкретного перечня иных процессуальных действий и описания порядка их проведения в УПК РФ. Это позволит упростить сбор информации и повысить эффективность уголовного процесса, а также обеспечит единство правоприменения на всей территории России.

Анализ УПК РФ позволяет выделить три группы способов, которые происходят из полномочий органов дознания, следствия и прокуратуры:

- получение объяснений у подозреваемого относительно возникшего подозрения за его согласием (пункт 2 части 4 статьи 46 УПК) относится к числу иных процессуальных действий, предусмотренных уголовно-процессуальным законодательством. Данное действие может быть проведено только с согласия подозреваемого и является дополнительной мерой, направленной на выяснение обстоятельств дела.

- направление требований, поручений, запросов, обязательных для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами в пределах полномочий, установленных УПК РФ (часть 4 статьи 21 УПК) не относится к числу иных процессуальных действий, а представляет собой общую полномочную основу для проведения следственных действий.

- приобщение к уголовному делу предметов, документов, справок и т.д., представляемых органам расследования и прокурору защитником на основании пункта 3 части 2 статьи 86 УПК РФ также относится к числу иных процессуальных действий. Данное действие может быть проведено защитником подозреваемого или обвиняемого только при условии, что эти материалы могут повлиять на исход дела. При этом, необходимо соблюдать требования уголовно-процессуального законодательства по обеспечению конфиденциальности и сохранности материалов, а также учитывать возможные ограничения на их использование в судебном разбирательстве.

Эти способы могут быть использованы в рамках уголовного процесса, чтобы получить необходимую информацию и доказательства. Важно отметить, что эти способы должны соответствовать законодательству и не нарушать права участников процесса.

Ко второй группе способов, которые обусловлены обязанностью субъектов доказывания обеспечить реализацию прав иных участников судопроизводства на сбор и представление документов и предметов для приобщения к уголовному делу, относятся:

1) принятие представляемых письменных документов и предметов, о приобщении которых ходатайствуют подозреваемый, обвиняемый и другие участники (ч. 2 ст. 86 УПК РФ).

2) получение материалов, представляемых специальными органами, уполномоченными на осуществление оперативно-розыскной деятельности (ст. 89 УПК РФ).

Эти способы необходимы для сбора и предоставления доказательств в уголовном процессе. Они также должны соответствовать законодательству и не нарушать прав участников процесса. Кроме того, субъекты доказывания несут ответственность за предоставление ложных документов и сведений.

К иным процессуальным действиям, которые осуществляются с целью получения доказательств в уголовном процессе, относятся:

1) оглашение показаний допрошенных на стадии предварительного расследования и в судебном заседании лиц. Это может быть использовано как один из способов получения доказательств. Показания могут использоваться для подтверждения фактов, установления обстоятельств дела и определения главных виновников.

2) получение объяснений на судебном разбирательстве от подсудимого, осужденного или оправданного (в суде второй инстанции). Объяснения могут использоваться для выяснения обстоятельств дела, а также для дополнительной информации от подсудимого и других участников процесса.

Также иными процессуальными действиями, направленными на получение доказательств, могли бы быть:

- 1) получение объяснений у граждан и должностных лиц;
- 2) принятие у граждан и должностных лиц документов, предметов и иных материальных объектов;
- 3) получение консультативного заключения специалиста;

4) назначение и производство документальной ревизии и документальной проверки;

5) истребование у должностных лиц, граждан, учреждений, организаций, предприятий предметов и документов, за исключением предметов и документов, для которых установлен особый режим хранения, передачи, пересылки, ознакомления¹.

Приведению УПК РФ в соответствие с потребностями правоприменительной практики и исключению ошибок по причине его несовершенства могли бы способствовать следующие дополнения и изменения.

1. Дополнение ст. 5 УПК РФ отдельным пунктом, содержащим толкование понятия «иные процессуальные действия», целью выполнения которых является получение доказательств.

2. Дополнение ст. 144 УПК РФ частью 1-а, в которой был бы определен перечень указанных иных процессуальных действий.

Таким образом можно сделать вывод: «иные процессуальные действия» по получению доказательств не должны быть такими же сложными, как следственные действия. Однако, они должны иметь четкое содержание и процедуру выполнения для обеспечения прозрачности и законности процесса.

Отсутствие конкретного перечня «иных процессуальных действий» и определения понятия может создавать некоторые проблемы в судебной практике. Так, для участников судопроизводства может быть неясно, когда, от кого и при каких обстоятельствах были получены те или иные факты и доказательства. Это может приводить к спорам и неопределенности в решении дел.

Тем не менее, необходимо учитывать, что любое процессуальное действие, направленное на получение доказательств, должно быть проведено в соответствии с требованиями уголовно-процессуального законодательства и

¹ Россинский С. Б. Собираение доказательств как первый этап доказывания по уголовному делу //Юридический вестник Самарского университета. 2020. №4. С.123-128.

только при наличии законных оснований. Кроме того, необходимо соблюдать правила по защите информации и конфиденциальности данных.

В целом, чтобы избежать неопределенности и споров в судебной практике, можно рассмотреть вопрос о введении конкретного перечня «иных процессуальных действий» и определения понятия в уголовно-процессуальном законодательстве. Это позволит обеспечить единообразие применения закона на всей территории России и упростить сбор информации для повышения эффективности уголовного процесса.

ГЛАВА 2. ОСОБЕННОСТИ ФИКСАЦИИ СЛЕДСТВЕННЫХ И ПРОЦЕССУАЛЬНЫХ ДЕЙСТВИЙ, ПРОВОДИМЫХ С ЦЕЛЬЮ ПОЛУЧЕНИЯ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ, ХРАНЯЩЕЙСЯ НА РЕСУРСАХ СЕТИ ИНТЕРНЕТ

§ 1. Особенности фиксации хода и результатов изъятия информации, сопряженной с ресурсами сети Интернет

Информация, размещенная в сети Интернет, имеет некоторые особенности, которые не присущи другим видам информации. Это связано с тем, что эта информация может параллельно существовать на различных носителях и быть доступна одновременно для большого числа пользователей.

Содержание сайта может храниться на разных носителях и использоваться различными пользователями. В связи с этим, при расследовании преступлений в сфере информационных технологий необходимо учитывать особенности сбора и анализа доказательств.

В первую очередь, необходимо обеспечить сохранность информации на компьютерных носителях, где хранится содержание сайта. При проведении обыска необходимо обращать внимание на наличие скрытых разделов

жесткого диска, зашифрованной информации и других методов скрyтия данных.

Кроме того, необходимо учитывать, что копии текстов, программного кода, изображений и других файлов могут использоваться разными пользователями. Для выявления подозреваемых и установления цепочки передачи информации могут использоваться методы анализа сетевых данных и метаданных, которые позволяют отслеживать передачу информации через сеть связи.

В целом, при расследовании преступлений в сфере информационных технологий необходимо использовать специализированные методы сбора, анализа и фиксации доказательств, учитывать специфические особенности цифровых данных, а также соблюдать требования уголовно-процессуального законодательства по обеспечению конфиденциальности и сохранности данных.

При обнаружении, фиксации и изъятии цифровой информации важно определить ее распространение и источник для установления ответственных лиц и получения более детальной информации о совершенном преступлении.

Для этого могут быть использованы специализированные программные и аппаратные средства, которые позволяют проводить мониторинг интернет-трафика и следить за передачей информации через сеть. Также могут быть применены методы анализа метаданных и цифровых следов, которые помогают выявлять цепочку передачи информации и определять ее источник.

Кроме того, необходимо проверить наличие данной информации на других сайтах или ресурсах. Для этого могут быть использованы поисковые системы и специализированные базы данных, которые помогают отслеживать размещение информации в Интернете.

Важным этапом является идентификация пользователей, которые могут иметь доступ к доказательственной информации, например, администраторов сайтов или пользователей, разместивших информацию в социальных сетях.

Это позволяет выявить подозреваемых и установить цепочку передачи информации.

В целом, при обнаружении, фиксации и изъятии цифровой информации важно проводить комплексную работу по определению ее распространения и источника. Для этого могут быть использованы различные методы анализа цифровых данных и специализированные программные и аппаратные средства. При выполнении процессуальных действий также необходимо соблюдать требования уголовно-процессуального законодательства по обеспечению конфиденциальности и сохранности данных.

Кроме текстовой информации, могут быть представлены мультимедийные файлы, такие как аудио-, видео- и изображения. Также криминалистически значимой информацией могут быть метаданные, которые могут содержать информацию о времени создания файла, местоположении устройства, использованном при создании файла, производителе устройства и т.д.

Для получения криминалистически значимой информации из Интернета необходимо проводить специальные исследования и экспертизы, так как она может быть скрыта или изменена. Кроме того, важно соблюдать законы и правила использования данной информации, чтобы она могла быть допустима в качестве доказательства в суде.

Для сбора и фиксации доказательственной информации в данном случае могут быть использованы специализированные программные и аппаратные средства, которые позволяют проводить мониторинг Интернет-трафика и собирать информацию о действиях пользователей в сети.

Важным этапом является установление цепочки передачи информации и источника данных. Для этого могут быть применены методы анализа метаданных и цифровых следов, которые помогают выявить цепочку передачи информации и определить ее источник.

При получении информации из телеконференций, вебинаров, чатов и других коммуникационных каналов необходимо учитывать требования

уголовно-процессуального законодательства по обеспечению конфиденциальности персональных данных и сохранности информации.

В целом, для успешного расследования преступлений связанных с Интернетом, необходимо использовать комплексный подход к сбору, фиксации и анализу доказательственной информации. Для этого могут быть использованы различные методы и специализированные программные и аппаратные средства.

Для того чтобы правильно закрепить информацию и превратить ее в доказательство, необходимо выполнить следующие требования:

Фиксация места и времени получения информации. Важно точно зафиксировать место и время получения информации, чтобы можно было подтвердить ее подлинность и надежность.

Правильное хранение информации. Полученную информацию необходимо сохранять в безопасном месте и в соответствии с требованиями закона.

Если информация требует экспертизы или анализа, то она должна быть передана на соответствующую экспертизу.

Документирование информации. Информация должна быть документирована в установленной форме, чтобы ее можно было использовать в качестве доказательства.

Процессуальная корректность фиксации интернет-информации включает не только описание содержания и реквизитов цифровой информации в протоколах осмотра, обыска или заключении эксперта, но также рекомендуется использовать дополнительные способы фиксации для увеличения достоверности доказательств.

Один из эффективных методов - это внесение скриншотов, распечаток логов, выдержек из внутренней или внешней аналитики и статистики по сайту и т.д. Эти материалы могут являться ценным дополнением к текстовому описанию, который иногда может не передать всю суть и значения информации.

Кроме того, включение понятых в процесс участия следственного осмотра или обыска может быть полезным, чтобы помочь разъяснить технические детали и терминологию, используемые специалистами и следователями при проведении данной работы. Такие действия способствуют лучшему пониманию технических аспектов и обеспечивают большую точность и достоверность доказательств, что в конечном итоге помогает ускорить расследование преступления и повысить качество собранных доказательств.

Корректность фиксации связи обнаруженной информации с расследуемым событием или личностью участника расследования является важнейшей частью процесса сбора доказательств в криминалистике.

Важно также отметить, что в отличие от многих других следов, которые изучает криминалистика, следовая информация, найденная в Интернете, может оставаться неизменной после ее изучения.

Таким образом, для обеспечения корректности фиксации связи обнаруженной информации с расследуемым событием или личностью участника расследования, следователь должен быть внимателен к деталям и описывать все действия и использованную технику и программное обеспечение с максимальной точностью.

При фиксации информации из Интернета в протоколе следует указывать наименование и версию браузера, а также перечислять и описывать все подключенные модули, дополнения и расширения, которые могут повлиять на отображение страницы и содержимого.

HTML является стандартизированным языком разметки документов в Интернете, то в целом, веб-страницы должны отображаться одинаково в разных браузерах. Однако, ввиду наличия собственных расширений и подключаемых модулей для обработки веб-содержимого, отображение страницы может отличаться в разных браузерах.

Например, некоторые браузеры могут блокировать определенные элементы страницы, показывать всплывающие окна или скрытые элементы, в то время как другие браузеры могут отображать их без изменений.

При обнаружении физического носителя информации в Интернете (например, сервера) необходимо выполнять дополнительные меры безопасности для обеспечения корректной фиксации доказательств и защиты целостности информации. Некоторые из этих мероприятий включают: Важно также обеспечить стабильность электроснабжения объекта осмотра и защитить устройство от возможных сбоев в электроснабжении. Для этого может быть полезным использовать бесперебойное питание (UPS), которое позволяет сохранять работоспособность устройства в случае временного прерывания электропитания.

Кроме того, необходимо провести тщательную проверку объекта осмотра на наличие скрытых коммуникационных каналов, которые могут использоваться для передачи информации о процессе обыска. Для этого могут быть использованы специализированные программы и аппаратные средства, которые позволяют обнаруживать скрытые камеры, микрофоны и другие устройства.

Важным аспектом обеспечения безопасности при проведении обыска является также соблюдение правил конфиденциальности и сохранности информации.

В целом, при проведении обыска необходимо использовать комплексный подход к обеспечению безопасности и сохранности информации, который включает в себя различные методы и средства безопасности. При выполнении процессуальных действий также необходимо соблюдать требования уголовно-процессуального законодательства по обеспечению конфиденциальности и сохранности данных.

Воспользоваться помощью специалиста в области сетевых технологий для обеспечения контроля над перемещением информации по сети.

Все эти мероприятия помогут обеспечить безопасность фиксации информации при обнаружении физического носителя в Интернете и обеспечить корректность доказательств в уголовном деле.¹

При расследовании преступлений в Интернете может потребоваться установление логинов, паролей, кодов доступа и других секретных данных, защищающих программы и базы данных.

Однако, полученные сведения не следует принимать только на слух. Важно записывать все сведения, которые могут помочь в расследовании дела, и соблюдать правильный регистр символов и язык их исполнения.

Таким образом, при расследовании преступлений в Интернете, с установлением логинов, паролей и других секретных данных, следует использовать осторожность, записывать полученные данные и связывать их с конкретным расследуемым событием для обеспечения корректности доказательств.

Перед отключением персонального компьютера или сервера от электропитания необходимо закрыть все запущенные приложения и провести некоторые мероприятия для обеспечения сохранности данных.

Сделать скриншоты или сфотографировать запущенные приложения или список процессов в диспетчере задач, чтобы иметь возможность восстановить их состояние в будущем, если это будет необходимо.

Провести осмотр и фиксацию любой документации, находящейся рядом с осматриваемым устройством. Это может включать краткие записки, планеры, визитки, записные книжки и другие предметы, которые могут быть связаны с расследуемым делом.

Дополнительно можно использовать другие методы для обеспечения сохранности данных, такие как копирование важных файлов, создание бэкапов или использование других средств для хранения данных. Однако, указанные

¹ Бахтеев Д. В. Особенности фиксации и изъятия криминалистически значимой информации, размещенной в сети интернет//Российский следователь. 2017. № 21. С.10-13.

мероприятия должны быть выполнены для обеспечения сохранности информации при последующей работе с устройством.

Таким образом, при осмотре персонального компьютера или сервера перед отключением от электропитания необходимо провести ряд мероприятий для обеспечения сохранности данных, включая закрытие приложений, создание скриншотов и фиксацию документации.

§ 2. Особенности следственного осмотра и фиксации информации, хранящейся на ресурсах сети Интернет

Протокол следственного осмотра (обыска), проводимого для фиксации информации, хранящейся на ресурсах сети Интернет, должен содержать описание ключевых характеристик изучаемых компьютерных устройств. Это поможет однозначно идентифицировать устройства и сохранить доказательственную ценность обнаруженной информации.

Для этого в протоколе должны быть указаны различимые частные признаки внешнего вида каждого устройства, такие как размеры, форма, цвет и другие характеристики. Это поможет не только идентифицировать устройства, но и произвести их дальнейшую экспертизу.

Кроме того, протокол должен содержать информацию о конфигурации и комплектации каждого устройства, включая процессор, оперативную память, жесткие диски, видеокарты и другие компоненты устройства. Эта информация поможет определить физические возможности устройства и возможности доступа к информации.

Важно также отметить, что протокол должен содержать максимально подробное описание всех действий, совершенных при проведении обыска, включая временные метки и имена всех присутствующих лиц. Это позволит установить цепочку действий и фиксировать нарушения правил проведения обыска.

В целом, протокол следственного осмотра (обыска) должен содержать подробную информацию об изучаемых компьютерных устройствах и всех действиях, совершенных при проведении обыска. Это поможет сохранить доказательственную ценность обнаруженной информации и соблюсти все требования уголовно-процессуального законодательства.

Формальные индивидуализирующие признаки, такие как серии и номера моделей, инвентарные номера и другие идентификационные данные, могут быть использованы для точного определения устройства. Эти данные могут быть указаны в протоколе следственного осмотра (обыска) и помочь в дальнейшей экспертизе устройства.

Идентификационные данные устройства могут помочь в установлении его производителя, модели, конфигурации и других характеристик. Это может быть полезно в контексте расследования преступлений, исследования технических проблем или оценки ценности устройства. Эксперты-криминалисты, инженеры или специалисты по информационной безопасности, могут использовать эти данные для более детального анализа и определения возможных связей или причинно-следственных связей.

Кроме того, сведения, содержащиеся на этикетках, наклейках, бирках и ярлыках фирмы-изготовителя, также могут содержать важную информацию о производителе, модели, серийном номере и других технических характеристиках устройства. Эта информация может быть использована для точной идентификации устройства и выявления его конфигурации и комплектации.

Важно отметить, что при проведении обыска необходимо быть внимательным к дополнительным деталям, которые могут использоваться для однозначной идентификации устройства. Например, это может быть номер лицензии операционной системы, адрес MAC-адреса и другие параметры.

Данные формы фиксации интернет-информации могут рассматриваться как допустимые, при условии соблюдения всех необходимых формальностей, таких как указание URL-адреса сайта, дата и время обращения к сайту и т.д.

Распечатанные скриншоты или страницы веб-сайта, в совокупности с рапортом сотрудника полиции, могут служить доказательствами в уголовном процессе.

Выбор формы доказательства интернет-информации зависит от конкретной ситуации и доступных ресурсов для фиксации информации. Для получения полноценных доказательств может потребоваться проведение дополнительных исследований и экспертиз.

Например, для фиксации информации на веб-странице может использоваться программа для сохранения веб-страницы в архивном формате или специальная служба, которая способна фиксировать изменения на веб-страницах. В некоторых случаях может потребоваться проведение лингвистической экспертизы текста для определения авторства.

Также могут применяться и другие методы, такие как запись снимков экрана, фиксация данных в лог-файлах сервера, анализ баз данных и другие. Важно подобрать наиболее подходящий метод для конкретной ситуации, исходя из требований уголовно-процессуального законодательства и доступных ресурсов.

Информация, которая предоставляется, может быть приобщена в качестве доказательства к материалам уголовного дела, однако приоритетной является именно следственная форма фиксации интернет-информации¹.

Изъятие информации, размещенной в сети Интернет, может восприниматься с разных сторон. С одной стороны, изъятию может подлежать носитель такой информации, например сервер, на котором физически размещается веб-сайт. Правила изъятия подобных объектов в целом аналогичны технологии изъятия вещественных доказательств. По возможности исследование сервера специалистом или экспертом следует организовать по месту нахождения сервера без его отключения от сети в целях

¹ Вехов В. Б. Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения: Сб. науч.-практ. тр. М.: Академия Следственного комитета Российской Федерации, 2016. № 1. С. 46 - 50.

сохранения содержимого оперативной памяти, например, с помощью мобильного компьютерного стенда. Если такая возможность отсутствует, то изъятие компьютера, сервера или кластера (объединенной группы) серверов необходимо производить следующим образом, который применяется в ОМВД по Уфимскому району Республики Башкортостан¹:

- выключить компьютер или отключить сервер. При этом следует вынимать вилку из розетки, а не выключать компьютер кнопкой питания либо переключением тумблера блока питания;

- отключить осматриваемое устройство от Интернета (если подключение осуществлялось с помощью кабеля);

- отсоединить все подключенные разъемы, опечатав каждый с помощью липкой ленты или клея длинной полосой бумаги с описанием номера, времени, места изъятия, характеристик изымаемого объекта, заверенной подписями следователя, специалиста и понятых;

- аналогичным образом опечатать разъемы на кабелях периферийных устройств;

- изъять и упаковать в отдельные контейнеры внешние носители информации, при этом следует учитывать, что оптические диски (CD, DVD, Blue-ray и т.п.) необходимо упаковать таким образом, чтобы исключить возможность их повреждения. Аналогичным образом упаковываются внешние жесткие диски и отключенные от компьютера жесткие диски. Твердотельные носители информации (флеш-карты, SSD-диски и т.п.) упаковываются в отдельные полиэтиленовые пакеты. Следует оградить изымаемые объекты от воздействия магнитных полей (не хранить и не транспортировать вместе с магнитными подъемниками, дактилоскопическими магнитными кистями и т.п.).

² Уголовное дело № 120018***** (расследование преступлений в сфере компьютерной информации) по ст. 159.6 УК РФ \\ Архивные данные ОМВД по Уфимскому району Республики Башкортостан. – 2020 год.

Соблюдение указанных требований помогает обеспечить эффективное исследование изъятых объектов, в том числе интернет-информации, в рамках следственного осмотра и компьютерно-технической экспертизы. Это позволяет достичь минимизации возможных противодействий технического характера со стороны заинтересованных лиц.

Вторым аспектом изучаемого вопроса является, когда информация, необходимая для следствия, находится в сети Интернет и изъять ее непосредственно не представляется возможным. Такое может произойти, если сервер с нужной информацией расположен в другом государстве, а также в случае отсутствия соглашения об оказании правовой помощи между этим государством и Российской Федерацией.

В данном случае речь идет о семантической информации, то есть о содержании сообщения, которое имеет значение для следствия само по себе. В таких случаях изъятие носителя информации может быть излишним и неэффективным.

Например, если на форуме или социальной сети было опубликовано экстремистское сообщение, то для его изучения достаточно получить доступ к самому сообщению, а не пытаться изъять сервер, на котором было размещено это сообщение. Доступ к самому сообщению можно получить через специальные программы для мониторинга интернет-среды, мониторинг аккаунтов подозреваемых лиц или другие методы.

Важно учитывать, что при использовании подобных методов следует соблюдать все требования уголовно-процессуального законодательства. Например, необходимо обеспечить сохранность доказательств и право на конфиденциальность переписки. Также следует учитывать, что при использовании программ для мониторинга интернет-среды необходимо учитывать их ограничения и возможности.

Тем не менее, при возникновении подобных ситуаций возможно применение других методов, например, запрос информации у провайдера

услуг хранения данных, который обязан предоставить запрашиваемые данные в соответствии с законодательством.

Таким образом, не всегда необходимо изымать носитель информации, размещенной в сети Интернет, при наличии необходимой семантической информации. В таких случаях возможны другие методы получения информации, которые следует использовать в соответствии с действующим законодательством. В подобных случаях изъятие следовой информации будет отличаться от изъятия традиционных криминалистических следов.

В соответствии со статьями 182 и 183 УПК РФ при копировании информации на электронные носители обязательно требуется участие специалиста. Это необходимо для сохранения целостности и достоверности изымаемой информации и ее использования в дальнейшем в качестве доказательства.

В протоколе следственного действия должна быть отметка об изъятии информации соответствующим способом и описание внешнего вида и технических характеристик носителя. Это поможет в дальнейшей экспертизе и анализе изъятой информации.

Важно учитывать, что процедура изъятия информации с электронных носителей должна проводиться в соответствии с требованиями уголовно-процессуального законодательства. Например, необходимо обеспечивать сохранность информации и использовать только специализированное оборудование для копирования данных.

Также при проведении изъятия информации с электронных носителей следует обращать внимание на общее состояние носителя и его технические характеристики. Например, если носитель поврежден или имеет другие дефекты, это может повлиять на качество изъятой информации и ее использования в дальнейшем в качестве доказательства.

В целом, при изъятии информации с электронных носителей необходимо учитывать требования уголовно-процессуального законодательства и обеспечивать сохранность и достоверность информации.

Описание внешнего вида и технических характеристик носителя должно быть включено в протокол следственного действия для дальнейшей экспертизы и анализа изъятой информации.

Важно отметить, что при копировании интернет-информации на другой цифровой носитель, например, внешний жесткий диск, флэш-накопитель или оптический диск, необходимо следить за тем, чтобы сохраненная информация была полной и точной копией оригинальной информации.

Таким образом, при изъятии компьютерной информации необходимо соблюдать все требования законодательства, включая участие специалиста при копировании информации на другой цифровой носитель, опечатывание этого носителя и составление пояснительной записки.

§ 3. Компьютерная экспертиза как средство доказывания при расследовании преступлений, совершенных с использованием сети Интернет

Результаты анализа состояния уровня преступности в России показывают, что количество зарегистрированных преступлений, совершённых с использованием информационно-телекоммуникационных технологий, с каждым годом увеличивается. Так, за 2017 год зарегистрировано 90 тыс. 587 преступлений совершённых с использованием компьютерных и телекоммуникационных технологий; за 2018 год — 174 тыс. 674 (+92,8 %); за 2019 год зарегистрировано 294 тыс. 409 (+68,5 %) преступлений, совершённых с использованием информационно-телекоммуникационных технологий. За период с января по ноябрь 2020 года зарегистрировано 461 тыс. 222 (+76,6 %) преступления, совершённых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации¹.

¹ Статистика. Состояние преступности в России за январь-декабрь 2017, 2018, 2019, январь — ноябрь 2020 г.

Совершение преступления с использованием сети Интернет может требовать обращения к специалистам, так как электронная информация является объектом и средством совершения преступлений, а ее осмотр и исследование требуют специальных знаний в соответствующей области.

Действительно, практически любое обращение с компьютерной информацией требует использования специальных знаний, чтобы оценить значение и содержание информации, определить ее целевое назначение и способ использования, а также выявить следы, оставленные при использовании электронных средств связи.

В связи с этим, экспертные исследования являются необходимой составляющей в расследовании преступлений, связанных с использованием сети Интернет. Такие исследования могут придать изъятым аппаратным средствам, программному обеспечению и компьютерной информации доказательственное значение, что может быть использовано в ходе судебного разбирательства.

Экспертные исследования проводятся специалистами в соответствующих областях, например, информационной безопасности, программирования и т.д. Они должны быть независимыми и объективными, чтобы результаты исследований могли быть использованы в качестве доказательств в судебном процессе.

Анализ материалов уголовных дел показывает, что компьютерная экспертиза активно используется в расследовании преступлений, совершённых с использованием сети Интернет. Однако назначается она, как правило, лишь в тех случаях, когда применение компьютерной техники и (или) информационно-телекоммуникационных сетей прямо указано законодателем в качестве квалифицирующего признака состава преступления либо обстоятельства, отягчающего ответственность¹.

¹ Определение Верховного суда РФ от 22.03.2018 № 303-ЭС17-16652 по делу № А73-8184/2016

Эффективность заключения компьютерной экспертизы как средства доказывания подтверждает её распространенное назначение при расследовании преступлений, совершённых с использованием сети Интернет: нарушение авторских и смежных прав в области системного программного обеспечения и аудио-видеоигровых носителей информации (ст. 146 УК РФ); кража с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ); мошенничество (ст. 159 УК РФ); мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ); мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) (например, в сфере компьютерной телефонии, мобильных платформ и платежей); публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма (ст. 205.2 УК РФ); незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества (ст. 228.1 УК РФ); незаконные изготовление и оборот порнографических материалов или предметов, в том числе с изображением несовершеннолетних (ст.ст. 242, 242.1 УК РФ) посредством сети Интернет; неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); публичные призывы к осуществлению экстремистской деятельности, совершённые с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет (ч. 2 ст. 280 УК РФ) и др.

Процесс назначения и производства компьютерной экспертизы может быть представлен следующими стадиями:

1. Определение наличия основания для назначения компьютерной экспертизы, например, если имеются основания полагать, что компьютерная информация является объектом или средством совершения преступления.

2. Выбор экспертного учреждения и вида (рода) назначаемой судебной экспертизы, в данном случае - компьютерной экспертизы.

3. Подготовка объектов, подлежащих направлению на компьютерную экспертизу, например, компьютерного оборудования или хранилища цифровой информации.

4. Формулирование вопросов для разрешения их экспертом, например, определение наличия скрытых данных или нарушений конфиденциальности.

5. Вынесение постановления о назначении компьютерной экспертизы судом.

6. Ознакомление подозреваемого, обвиняемого, его защитника, потерпевшего, его представителя с постановлением о назначении компьютерной экспертизы.

7. Направление постановления о назначении компьютерной экспертизы в экспертное или иное учреждение.

8. Производство компьютерной экспертизы, которое включает сбор, анализ и оценку цифровой информации, хранящейся на объектах, направленных на экспертизу.

9. Оформление заключения компьютерной экспертизы и передача его следователю, в котором должны быть детально описаны все обнаруженные за время экспертизы особенности и доказательства.

10. Ознакомление заинтересованных лиц с заключением компьютерной экспертизы, таких как подозреваемый, обвиняемый, его защитник, потерпевший, его представитель, чтобы они могли использовать это заключение в своих интересах.

Что такое компьютерная экспертиза?

Компьютерная экспертиза - это вид судебной экспертизы, который проводят специалисты в области информационных технологий для определения наличия или отсутствия информации на электронных носителях данных. Она может быть произведена как в государственных экспертно-

криминалистических подразделениях органов внутренних дел, так и в негосударственных экспертных организациях.

На каких носителях информации может храниться компьютерная информация?

Компьютерная информация может храниться на различных машинных носителях, таких как жесткие диски, гибкие магнитные диски, CD- и DVD-диски, flash-накопители, картах памяти и прочих носителях информации, имеющих файловую систему.

Какой вид информации относится к компьютерной информации?

Компьютерная информация - это информация, которая хранится на машинных носителях в системе ЭВМ или их сети. Она имеет материальную природу и представляет собой электромагнитное поле. Компьютерная информация является особым видом информации, который требует специальных знаний для ее обработки и использования.

Чем отличается компьютерная экспертиза от компьютерно-технической экспертизы?

Компьютерная экспертиза проводится экспертно-криминалистическими подразделениями органов внутренних дел Российской Федерации и направлена на выявление факта хранения или удаления конкретной информации на машинных носителях. Компьютерно-техническая экспертиза производится судебно-экспертными учреждениями системы Министерства юстиции Российской Федерации и оценивает технические аспекты работы программного обеспечения или оборудования.

Исходя из выше сказанного, компьютерная экспертиза направлена на выявление фактов совершения преступлений с использованием компьютеров и Интернета, а также на изучение цифровых следов, оставленных преступниками. Она может включать в себя анализ компьютерных систем, изучение логов и журналов операционных систем, а также изучение электронных сообщений и файлов.

Компьютерно-техническая экспертиза направлена на выявление технических характеристик и особенностей оборудования и программного обеспечения, используемых для работы с цифровой информацией. Она может включать в себя анализ аппаратных и программных средств, проверку соответствия требованиям безопасности и защиты информации, а также выявление нарушений законодательства в области информационной безопасности.

Перечень типичных вопросов, разрешаемых в рамках компьютерной экспертизы, зависит от обстоятельств исследуемого преступного события и направляемых на экспертизу материалов.

Так, например, к диагностическим вопросам о факте наличия или отсутствия тех или иных следов (в том числе электронных) совершения конкретных действий с информацией, хранящейся на электронно-вычислительном устройстве, могут быть отнесены следующие:

- имеются ли на предоставленном объекте файлы с текстовой информацией, содержащие ключевые слова (например, TheBottle, Yello, Quatra, Serj ivonov, <http://vk.com/id224173411>, Иванов Сергей Сергеевич, bhf.io, ifud.ws, yougame.biz, lolzteam.net, stealer, стиллер, граббер, steamstealer, Mining-Station, Project odysseus, Ovidiy Stealer, Reborn Stealer, Evrial Stealer, Eredel Stealer Lite, Eredel Stealer Full (extended), 9131313131, 9141414141, Qiwi-кошельки;

- имеется ли на предоставленном объекте установленная программа для общения Telegram (Skype, iMessage, Viber, Line, WhatsApp, Threema, Confide, Wickr, Signal и др.)? Если да, то какие пользователи зарегистрированы? Имеются ли сообщения переписки;

- имеются ли на объекте исследования компьютерные программы либо иная компьютерная информация, заведомо предназначенные для (скрытного от пользователя) уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

– имеются ли на объекте исследования признаки, указывающие на способ и время появления (распространения) компьютерных программ либо иной компьютерной информации, предназначенных для (скрытного от пользователя) уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации? Каков функционал обнаруженной компьютерной программы? Для каких целей предназначена обнаруженная компьютерная информация;

– имеются ли следы и (или) признаки взаимодействия обнаруженных на объекте исследования компьютерных программ либо иной компьютерной информации, предназначенных для (скрытного от пользователя) уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, с какими-либо и иными электронно-вычислительными машинами, сетевыми адресами, доменными именами;

– имеются ли на НЖМД, входящем в состав ноутбука DELL модель Precision 5550, сведения о зарегистрированных файлах, содержащих данные о посещении сайтов сети интернет-ресурсов за период с «_»__21 года по «_»__21 года;

– имеются ли на представленных объектах компьютерные программы, детектируемые антивирусным программным обеспечением как вредоносные?

Что такое постановка вопроса идентификационного характера в компьютерной экспертизе?

Постановка вопроса идентификационного характера в компьютерной экспертизе - это запрос, направленный на установление соответствия стилю программирования исследуемого программного продукта стилю программирования подозреваемого лица. Это достаточно необычная задача для компьютерной экспертизы, обычно такие запросы направлены на установление принадлежности различных цифровых объектов конкретным лицам.

Как организовывается процесс назначения и проведения компьютерной экспертизы?

Для назначения и проведения компьютерной экспертизы следователь составляет соответствующее постановление, в котором указывает цель и задачи экспертизы. В этом документе также указывается возможность редактирования экспертом, производящим исследование, поставленных для разрешения вопросов без изменения их смыслового содержания.

После составления постановления следователь знакомит с ним подозреваемого, обвиняемого, его защитника, потерпевшего, его представителя и разъясняет им права, предусмотренные статьей 198 УПК РФ. Кроме того, результаты исследования материалов практики показали, что правоприменитель идет по пути более широкого толкования круга участников уголовного судопроизводства, которым при назначении и производстве судебной экспертизы следует разъяснять права.

Для проведения компьютерной экспертизы могут быть направлены дополнительные запросы в банк, оператора сотовой связи, провайдера для сопоставления с результатами экспертизы. После этого следователь направляет постановление о назначении и производстве компьютерной экспертизы в ЭКЦ ГУВД (УМВД) субъекта Российской Федерации для проведения экспертизы.

В компьютерной экспертизе производство осуществляется на общих методических положениях и подходах. В процессе экспертного исследования сначала тщательно изучаются объекты экспертизы, анализируются их общие и частные признаки и свойства. Выполняются экспертные опыты и выясняются обстоятельства произошедшего, учитывая характер отображения исследуемых цифровых следов.

После этого происходит решение диагностических и идентификационных задач. Например, для решения идентификационной задачи, такой как поиск файлов по образцу, проводится сравнение хеш-сумм

файлов. Если они совпадают, можно утверждать об их идентичности по содержанию.

На стадии оценки результатов исследования подводятся итоги и формулируются выводы компьютерной экспертизы, логически вытекающие из проведенных исследований. В целом, процесс экспертного исследования в компьютерной экспертизе требует тщательного анализа и изучения объектов, проведения опытов и решения задач, чтобы достичь точных результатов.

Получив заключение компьютерной экспертизы, следователь, в соответствии со ст. 206 УПК РФ, предъявляет потерпевшему, его представителю, подозреваемому, обвиняемому, его защитнику, которым разъясняется при этом право ходатайствовать о назначении дополнительной либо повторной судебной экспертизы.

Основными проблемами при назначении компьютерной экспертизы и использовании её результатов в доказывании при расследовании преступлений, совершённых с использованием сети Интернет, является:

- низкий уровень общих технических знаний следователя о функционировании современной техники, информационно-телекоммуникационных сетей и информационных технологий;
- некорректное определение видов назначаемых судебных экспертиз;
- неправильное формулирование вопросов для разрешения экспертом;
- установление компетентности конкретного эксперта, которому поручается производство компьютерной экспертизы;
- ненадлежащая оценка полученного заключения компьютерной экспертизы на предмет его относимости и допустимости в качестве доказательства по уголовному делу.

Проблемы производства компьютерной экспертизы имеют как объективный, так и субъективный (зависящий от эксперта) характер. Некоторые из объективных проблем возникают еще до непосредственного производства экспертизы.

Одной из главных трудностей является то, что цифровые следы преступлений могут быть легко изменены или удалены без оставления видимых следов в физическом мире. Кроме того, такие следы могут быть зашифрованы или скрыты за сложными системами защиты.

Еще одна проблема заключается в том, что цифровые следы могут храниться на различных устройствах и серверах, которые расположены в разных странах и под юрисдикцией разных правовых систем, что требует международного сотрудничества и соответствующих документов и соглашений.

Также следует отметить, что цифровые следы не всегда имеют криминалистическую значимость, поскольку они могут быть случайными или созданными без намерения совершить преступление. Поэтому важно правильно определить, какие цифровые следы являются релевантными для дела и как их следует анализировать.

Для преодоления этих трудностей и обеспечения качественного производства компьютерных экспертиз необходимо обладать высокой технической и методологической компетенцией. Следователи должны знать основы работы с компьютерами и операционными системами, иметь навыки анализа кода и программного обеспечения, понимать принципы шифрования и защиты информации, уметь работать с базами данных и сетевыми протоколами.

Кроме того, следователи должны иметь доступ к квалифицированным компьютерным экспертам и использовать современное программное обеспечение для обработки цифровых следов.

Таким образом, важно развивать и усовершенствовать систему подготовки и обучения следователей по компьютерной криминалистике, обеспечивать доступ к квалифицированным экспертам и использовать современные технологии и методы для производства компьютерных экспертиз.

Исходя из вышеизложенного, считаем необходимым уточнить содержание ст. 86 УПК РФ в части терминологического определения собирания доказательств:

«Собирание доказательств представляет собой начальный этап доказывания, осуществляемый в ходе уголовного судопроизводства дознавателем, следователем, прокурором и судом путем производства следственных и иных процессуальных действий, предусмотренных настоящим Кодексом».

Дополнение ст. 5 УПК РФ отдельным пунктом, содержащим толкование понятия «иные процессуальные действия», целью выполнения которых является получение доказательств.

Дополнение ст. 144 УПК РФ частью 1-а, в которой был бы определен перечень указанных иных процессуальных действий.

Нужно также в УПК РФ регламентировать новое следственное действие - проверку показаний на полиграфе, для того чтобы получить дополнительные достоверные доказательства.

ЗАКЛЮЧЕНИЕ

Согласен с тем, что статус следователя как субъекта доказывания является важным и неоспоримым. Следователь играет ключевую роль в процессе сбора, систематизации и проверки доказательств, которые будут использоваться в судебном процессе. Качество собранных доказательств и их соответствующее оформление могут определить ход дела и судьбу подсудимого.

Одним из основных способов сбора и проверки доказательств являются следственные действия, которые проводятся только лицом, в производстве которого находится уголовное дело, а также надзирающим прокурором. Важно учитывать, что следственные действия должны быть проведены в соответствии с законом и обеспечивать сохранность и достоверность собранных доказательств.

Процессуальное законодательство РФ не содержит единого понятия следственного действия, поэтому законодателю необходимо разрешить этот пробел и уточнить сущность и понятие собирания доказательств.

Дополнения и изменения в УПК РФ, такие как определение понятия "иные процессуальные действия" и перечень указанных действий, а также регламентация нового следственного действия - проверки показаний на полиграфе, могут способствовать улучшению правоприменительной практики.

Важно отметить, что сбор доказательств, размещенных в интернете, требует тактической и технической компетенции следователя. Экспертные исследования являются необходимыми для придания изъятых аппаратных средств, программного обеспечения и компьютерной информации доказательственного значения.

Однако проблемами при назначении компьютерной экспертизы и использовании ее результатов в доказывании при расследовании преступлений, совершенных с использованием сети Интернет, могут стать недостаточные технические знания следователя, неправильное формулирование вопросов для разрешения экспертом и неправильная оценка заключения компьютерной экспертизы.

Таким образом, совершенствование системы следственных действий должно быть направлено на уточнение и определение понятий, регламентацию новых следственных действий и повышение компетенции следователей в области сбора и проверки доказательств, включая использование экспертных исследований и сбор информации из интернета.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). Доступ из справ.-правовой системы «КонсультантПлюс».
2. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 нояб. 2001 г.: одобрен Советом Федерации Федер. Собр. Рос. Федерации 5 дек. 2001 г. // Собр. законодательства Рос. Федерации. 2001. № 52 (ч. 1), ст. 4921.

II. Учебная, научная литература и иные материалы

1. Арсентьева С. С. Проверка показаний на месте: Криминалистический анализ следственного действия, этические аспекты уголовно-процессуальной деятельности проверки и оценки данного доказательства // Российский судья. 2020. № 2. С. 27 - 32.
2. Бахтеев Д. В. Особенности фиксации и изъятия криминалистически значимой информации, размещенной в сети интернет // Российский следователь. 2017. № 21. С. 10-13.
3. Вехов В. Б. Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения: Сб. науч.-практ. тр. М.: Академия Следственного комитета Российской Федерации, 2016. № 1. С. 46 - 50.
4. Елагина Е. А. Перспективы развития системы следственных действий // Сборник научных статей 3-й Международной научной конференции студентов и молодых ученых. – Курск: Закрытое акционерное общество Университетская книга, 2018. С. 159- 162.

5. Коновалова А. Б., Гук А. Г. Следственные действия как способы собирания доказательств в досудебном производстве // Студент. 2021. №143. С. 59-64.
6. Манова Н. С., Францифоров Ю. В. Уголовный процесс. Учебное пособие. – М.: Юрайт, 2020. 244 с.
7. Пивоварова А. О. Проблемы собирания доказательств субъектами доказывания в уголовном судопроизводстве // Молодой ученый. 2018. № 27. С. 110–113.
8. Ромашко А. Н. Место следователя среди субъектов доказывания в уголовном процессе / А. Н. Ромашко. – Текст : непосредственный // Новый юридический вестник. 2020. № 1 (15). С. 29-32. – URL: <https://moluch.ru/th/9/archive/151/4728/> (дата обращения: 10.11.2022).
9. Россинский С. Б. Собирание доказательств как первый этап доказывания по уголовному делу //Юридический вестник Самарского университета. 2020. №4. С. 123-128.
10. Сафронов Д. М. Уголовно-процессуальные и криминалистические аспекты получения информации о пользователях сети Интернет при производстве следственных действий // Российская юстиция. 2021. № 1. С. 30 - 33.
11. Семенов Е. А. Правовое положение некоторых неуказанных в гл. 5-8 УПК РФ субъектов уголовного судопроизводства России. М.: НОРМА, 2020. С. 155.
12. Скобелкина К.С. Следственные действия, основанные на визуальных наблюдениях и опытных действиях // Трибуна ученого. 2020. № 2. С. 130 -138.

III. Эмпирические материалы

1. Определение Верховного суда РФ от 22.03.2018 № 303-ЭС17-16652 по делу № А73-8184/2016 // Справ.-правовая система «Консультант плюс» [Электронный ресурс]. — URL: base.consultant.ru (дата обращения: 12.01.2021).
2. Уголовное дело № 120018***** по ст. 159.6 УК РФ \\ Архивные данные ОМВД по Уфимскому району – 2020 год.
3. Статистика. Состояние преступности в России за январь-декабрь 2017, 2018, 2019, январь – ноябрь 2020 гг. [Электронный ресурс]. – URL: <https://мвд.рф/reports/1/> (дата обращения: 10.11.2022).

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну.

Д.А. Садыков